

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-55164

(43) 公開日 平成8年(1996)2月27日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 17/60				
13/00	3 5 1 H	7368-5E		
	Z	7368-5E		
G 0 9 C 1/00		7259-5J		
G 0 6 F 15/ 21 Z				
審査請求 未請求 請求項の数7 書面 (全 12 頁)				

(21) 出願番号 特願平6-219369

(22) 出願日 平成6年(1994)8月10日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中1015番地

(72) 発明者 秋山 良太

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中1015番地

富士通株式会社内

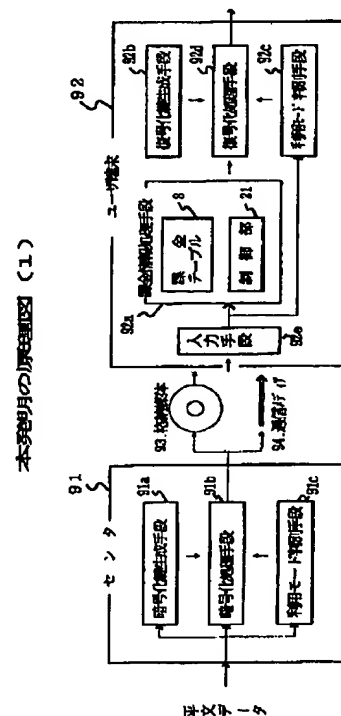
(74) 代理人 弁理士 遠山 勉 (外1名)

(54) 【発明の名称】 ソフトウェア配送システム、中継装置およびユーザ端末装置

(57) 【要約】

【目的】 ソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現する。

【構成】 所定のソフトウェアを暗号化してユーザへ提供するセンタとユーザ端末とを備えておき、前記センタおよび中継装置は、ソフトウェア供給形態にとって最適なモードでの暗号化を行うようにした。



1

【特許請求の範囲】

【請求項 1】 ソフトウェアを暗号化してユーザ端末に提供し、ユーザはソフトウェアの利用形態に応じて料金を支払うシステムであって、
所定のソフトウェアを暗号化してユーザへ提供するセンタとユーザ端末とを備え、
前記センタは、ユーザが希望するソフトウェアの属性に従って、このソフトウェアを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、
前記ソフトウェアの特性に基づいて暗号化のモードを決定する利用モード判別手段と、
前記暗号化鍵生成手段が生成した暗号化鍵及び前記利用モード判別手段が判別したモードに従って、前記ソフトウェアを暗号化する暗号化処理部とを具備し、
前記ユーザ端末は、前記センタからソフトウェアを提供されたときに、ユーザの課金情報に基づいて前記ソフトウェアの復号化を許可すべき否かを判別する課金情報処理手段と、
前記ソフトウェアの属性に基づいてこのソフトウェアを復号化するための復号化鍵を生成する復号化鍵生成手段と、
前記ソフトウェアのモードを判別する利用モード判別手段と、
前記復号化鍵生成手段が生成した復号化鍵及び前記利用モード判別手段が判別したモードに基づいて前記ソフトウェアを復号化する復号化処理手段とを具備することを特徴とするソフトウェア配送システム。

【請求項 2】 請求項 1 において、課金処理手段は、ユーザが利用可能な残高値を登録した課金情報記憶手段と、
前記課金情報記憶手段を参照して残高値が特定値以上であるか否かを判別し、特定値以上ならばデータの復号化を許可すると同時に、前記課金情報記憶手段の残高を減算する制御部とを備えることを特徴とするソフトウェア配送システム。

【請求項 3】 請求項 1 において、前記暗号化鍵生成手段、及び前記復号化鍵生成手段は、前記ソフトウェアを個々に特定するソフトウェア ID、あるいは前記ソフトウェアのタイトルを検出し、これらの情報に基づいて暗号化鍵及び復号化鍵を生成することを特徴とするソフトウェア配送システム。

【請求項 4】 請求項 1 において、前記センタの利用モード判別手段は、前記ソフトウェアのモードを決定する際に、前記ソフトウェアの特性を参照すると同時に、前記ソフトウェアを格納媒体に格納して提供するかあるいは通信を経由して提供するかを判別し、この判別結果を参照してモードを決定することを特徴とするソフトウェア配送システム。

【請求項 5】 請求項 1 において、前記センタと前記ユーザ端末との間に設けられた中継装置であって、

2

前記中継装置は、前記センタで暗号化されたソフトウェアを復号化するための復号化鍵を生成する復号化鍵生成と、
前記センタから供給されるソフトウェアのモードを判別する入力側利用モード判別手段と、
前記復号化鍵及びモードに基づいて前記ソフトウェアを復号化する復号化処理手段と、
前記復号化されたデータを暗号化するための暗号化鍵を生成する暗号化鍵生成手段と、
前記ソフトウェアの特性に基づいて暗号化のモードを決定する出力側利用モード判別手段と、
前記暗号化鍵及び前記モードに基づいて前記ソフトウェアを暗号化する暗号化処理手段とを備えることを特徴とする中継装置。

【請求項 6】 前記請求項 5 の中継装置は、
前記センタから提供されたソフトウェア情報の暗号化モードを判別する利用モード判別手段と、
前記モードに基づいて当該ソフトウェア情報を復号化するための復号化処理手段と、
前記ユーザ端末に提供するソフトウェア情報の提供形態の特性に基づく特有のモードで前記ソフトウェア情報を再度暗号化する暗号化処理手段とを備えていることを特徴とする中継装置。

【請求項 7】 通信または媒体で提供された暗号化または非暗号化ソフトウェア情報を再生するとともに、そのソフトウェアの利用に応じた課金を実行するユーザ端末であって、

通信または媒体の種類によって入力経路を切り替える入力切り替え手段と、

暗号化ソフトウェア情報の復号と当該ソフトウェア情報の利用量に応じた課金を管理するソフトウェア管理手段と、

前記ソフトウェア管理手段から出力された復号情報を可視的・可聴的なデータに変換する情報変換部と、

前記ソフトウェア管理手段の前段に設けられ暗号化ソフトウェア情報を前記ソフトウェア管理手段に出力し、非暗号化ソフトウェア情報を前記情報変換部に出力する出力経路切り替え手段とからなるユーザ端末。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、コンピュータプログラムあるいは映像著作物等のソフトウェア、特にデジタル情報化されたソフトウェアの流通システムに適用して有効な技術に関する。

【0002】

【従来の技術】 CD-ROM や MO 等の大規模記憶媒体や、B-ISDN 等の大容量の高速通信技術、あるいはケーブルテレビ等の技術が発達してくると、これらの手段を用いてコンピュータプログラムは勿論、画像や音声デジタル情報として流通されることが予想される。

50

【0003】すなわち、従来ビデオテープで供給されていたような映像著作物がそのままCD-ROM等の格納媒体に格納されて販売されたり、またはCD-ROMのインタラクティブ性（双方向性）を利用したゲームとして市場に流通し始めてきている。

【0004】また、通信回線についても同様であり、前記のような映像著作物が通信を経由してユーザの手元に届けられる状況になってきている。ところで、この種のデジタル情報は他の媒体への複写が極めて容易であり、かつアナログ情報のような複写による劣化がないことから、同一情報の複製が可能であり、これらの行為により製造者の利益が害される可能性が極めて高い。すなわち、大容量の書換え可能な光磁気ディスクや磁気ディスク装置さえ所有していればわずかなDOSのコマンドの知識のみでCD-ROMの内容を複写することが簡単であった。

【0005】このように、十分なセキュリティチェックが不可能であることを理由にこの種のデジタル情報媒体のレンタル行為は製造者によって禁止されている場合が殆どである。

【0006】しかしながら、エンドユーザとしては現在のこの種のソフトウェアの価格は高額であり、本当にそのソフトウェアが自身の欲しているものと一致するか、あるいは自身の所有しているハードウェアで使用可能かの確認がとれるまでは購入を躊躇する場合が多い。

【0007】この点について、機能が制限されている多数のソフトウェアをCD-ROMに格納して安価に販売し、エンドユーザはそこから希望するソフトウェアについて代金を送金することにより機能制限を解除するコードを通知されるという新しいソフトウェアの流通方式が実現され始めている。

【0008】また、放送の分野においては、放送局から通信衛星を経由してユーザへ映像著作物を提供する方式が実現されている。この方式では、放送局と契約を交わしているユーザのみに映像著作物を提供するために、通信衛星からユーザに提供する情報を暗号化し、契約ユーザには解読器を提供する。そして、通信衛星から暗号化された情報を復号化するための鍵を送信し、解読器は鍵に基づいて情報を復号化する。これにより、契約ユーザは、復号化された映像情報を家庭用のテレビで視聴することができる。しかし、料金体系は、ユーザの視聴時間等に関係なく、一律の料金を支払う方法を採用しており、さらに、放送というメディアの片方向性によりユーザは放送局が決定した放送プログラムに拘束されるという問題がある。つまり、ユーザは、自身の希望する情報を視聴するためには、放送局が決定した時刻まで待たなければ視聴できないという問題がある。

【0009】

【発明が解決しようとする課題】そこで、本発明は、少なくとも、画像や音声を提供するセンタと、CD-ROM

MやMO等のソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現するために有効な技術を提供し、セキュリティの向上とユーザにかかる時間的な負担の軽減とを図ることを課題とする。

【0010】

【課題を解決するための手段】本発明は、前記課題を解決するために以下のようにした。これを図1に沿って説明する。

【0011】まず、本発明のソフトウェア配送システムは、センタ91とユーザ端末92とから構成されている。そして、センタ91は、ユーザが希望するソフトウェアを暗号化する機能を有している。詳細には、センタ91は、暗号化鍵生成手段91a、利用モード判別手段91c、及び暗号化処理手段91bを備えている。

【0012】暗号化鍵生成手段91aは、ソフトウェアを暗号化するための暗号化鍵を生成する機能を有している。利用モード判別手段91cは、ソフトウェアの特性に応じて暗号化のモードを決定する機能を有している。

【0013】暗号化処理手段91bは、暗号化鍵情報とモードに基づいてソフトウェアを暗号化する機能を有している。次に、ユーザ端末92は、センタ91から提供されるソフトウェアを復号化して出力する機能を有している。詳細には、ユーザ端末92は、課金情報処理手段92a、復号化鍵生成手段92b、利用モード判別手段92c、及び復号化処理手段92dを備えている。

【0014】課金情報処理手段92aは、各ユーザが使用できる金額を登録した課金テーブル8（課金情報記憶手段）と、ソフトウェア提供時に課金テーブル8の残高値が特定値以上であるか否かを判別し、特定値以上であれば、ソフトウェアの復号化を許可する制御部921とを備えている。

【0015】さらに、制御部921は、復号化を許可したソフトウェアについて、タイトル毎に課金を行う機能を有している。具体的には、ソフトウェアのタイトルを検出し、且つこのタイトルのソフトウェアの復号化を許可する度に、課金テーブル8の残高を減算していく。

【0016】復号化鍵生成手段92bは、ソフトウェアを復号化するための復号化鍵を生成する機能を有している。利用モード判別手段92cは、センタ91から提供されたソフトウェアのモードを判別する機能を有している。

【0017】さらに、復号化処理手段92dは、課金情報処理手段92aが復号化を許可した場合に限り、復号化鍵生成手段92bが生成した復号化鍵と利用モード判別手段92cが判別したモードとに基づいてソフトウェアを復号化するものである。

【0018】また、前述の暗号化鍵生成手段91aと復号化鍵生成手段92bとは、個々のソフトウェアを特定するソフトウェアID、あるいはソフトウェアのタイト

ル等の情報を検出し、これらの情報に基づいて暗号化鍵及び復号化鍵を生成するようにしてもよい。

【0019】ここで、センタ 91 からユーザ端末 92 へソフトウェアを提供する方法として、CD-ROM や MO 等の格納媒体 93 にソフトウェアを格納して提供する方法や、通信回線等の通信メディア 94 を経由して提供する方法等がある。これに応じて、センタ 91 は、ソフトウェアを格納媒体 93 へ書き込む機能と、ソフトウェアを送信する機能とを備えるようにする。そして、センタ 91 の利用モード判別手段 91c は、ソフトウェアを格納媒体 93 によりユーザへ提供するのか、あるいは通信メディア 94 を介してユーザへ提供するのかを判別し、この判別結果に基づいて暗号化のモードを決定するようにしてもよい。

【0020】また、本発明のシステムには、センタ 91 とユーザ端末 92 との間に、図 2 に示すような中継装置 95 を設けるようにしてもよい。この中継装置 95 は、センタ 91 から格納媒体 93 あるいは通信メディア 94 を利用して提供されたソフトウェアを、さらに単数または複数のユーザ端末 92 へ送信する機能を有している。具体的には、中継装置 95 は、復号化鍵生成手段 95a、入力側利用モード判別手段 95c、復号化処理手段 95b、暗号化鍵生成手段 95d、出力側利用モード判別手段 95e、暗号化処理手段 95f とを備える。

【0021】ここで、復号化鍵生成手段 95a は、センタ 91 から供給されたソフトウェアを復号化するための復号化鍵を生成する機能を有している。入力側利用モード判別手段 95c は、センタ 91 から供給されたソフトウェアの暗号化モードを判別する機能を有している。

【0022】復号化処理手段 95b は、復号化鍵生成手段 95a が生成した復号化鍵と入力側利用モード判別手段 95c が判別したモードとに基づいてソフトウェアを復号化するものである。

【0023】暗号化鍵生成手段 95d は、復号化されたソフトウェアを暗号化するための暗号化鍵を生成する機能を有している。出力側利用モード判別手段 95e は、ソフトウェアの特性に基づいて暗号化のモードを決定するものである。

【0024】暗号化処理手段 95f は、暗号化鍵とモードとに基づいてソフトウェアを暗号化する機能を有している。次に、本発明のユーザ端末について説明する。

【0025】本発明のユーザ端末 92 は、入力装置 92e、課金情報処理手段 92a、復号化鍵生成手段 92b、利用モード判別手段 92c、及び復号化処理手段 92d を備えている。

【0026】入力装置 92e は、ユーザが希望するソフトウェアを入力するものであり、例えば、格納媒体 93 からソフトウェアを読み込むドライブ装置、あるいは通信メディア 94 を介して送信されてくるソフトウェアデータを受信する通信装置等である。

【0027】課金情報処理手段 92a は、ソフトウェアが入力されたときに、ユーザの課金残高を参照し、ソフトウェアの復号化を許諾するか否かを判別する機能を有している。具体的には、ユーザが使用可能な金額を登録した課金テーブル 8 と、この課金テーブル 8 を参照して残高が特定値以上であるか（または“0”でない）否かを判別して特定値以上ならば（“0”でなければ）ソフトウェアの復号化を許可する制御部 921 とを備えている。

【0028】復号化鍵生成手段 92b は、ソフトウェアを復号化するための復号化鍵を生成する機能を有している。具体的には、ソフトウェアのソフトウェア ID やタイトル等に基づいて復号化鍵を生成する。

【0029】利用モード判別手段 92c は、入力されたソフトウェアのモードを判別する機能を有している。復号化処理手段 92d は、課金情報処理手段 92a がソフトウェアの復号化を許諾した場合に限り、復号化鍵生成手段 92b が生成した復号化鍵及び利用モード判別手段 92c が判別したモードに基づいてソフトウェアを復号化する機能を有している。

【0030】

【作用】本発明のソフトウェア配送システムでは、センタ 91 は、ユーザが希望するソフトウェアを暗号化し、ユーザへ提供する。つまり、センタ 91 は、ソフトウェアのソフトウェア ID やタイトル等に基づいて暗号化鍵を生成すると共に、ソフトウェアのデータ構造等に基づいて暗号化のモードを決定する。そして、センタは、暗号化鍵とモードとに基づいてソフトウェアを暗号化する。

【0031】センタで暗号化されたソフトウェアは、格納媒体 93 や通信メディア 94 によりユーザ端末 92 へ提供される。ユーザ端末 92 では、センタ 91 からソフトウェアが提供されたときに、ユーザの課金残高を参照し、残高が特定値以上（“0”でない）ならばソフトウェアの復号化を許諾する。そして、許諾したソフトウェアのタイトル毎にユーザの課金残高を減算する。次に、ユーザ端末 92 は、ソフトウェアのソフトウェア ID あるいはタイトル等に基づいて復号化鍵を生成すると共に、このソフトウェアのモードを判別する。ユーザ端末 92 は、復号化鍵とモードとに基づいてソフトウェアを復号化し、ディスプレイやスピーカ等の出力装置へ出力する。

【0032】本発明によれば、通信あるいは媒体といったソフトウェアの提供形態がいなかる場合であっても、統一的にソフトウェアの流通を管理することができる。また中継装置を設けて提供形態の変更を可能とすることによって、最適な提供形態でのソフトウェアの流通を実現できる。

【0033】

【実施例】本実施例において、センタ 91 と、中継装置

95と、ユーザ端末92とはほぼ同様のハードウェア構成で実現することができる。

【0034】図3は、その一例としてのユーザ端末の内部構成を機能ブロック図で示したものである。同図において、切り替えスイッチ57(SW1)は、入力インターフェースとしても機能し、通信回線51、CD-ROM52等の種々の提供経路からのソフトウェア情報を入力する。また、この切り替えスイッチ57(SW1)には、図示しない光磁気ディスクドライブ装置を通じて光磁気ディスク58へのソフトウェア情報の読み書きが可能となっている。

【0035】切り替えスイッチ57(SW1)の次段には、信号処理手段としての受信装置58、MO変調器59およびCD/MO復調器60が配置されている。受信装置58は、通信回線51からの受信信号として提供されたソフトウェア情報を本装置で取り扱い可能なデータ形式に変換するためのものであり、MO変調器59は光磁気ディスク58への書き込みを行うための変調手段である。また、CD/MO復調器60はCD-ROM52または光磁気ディスク58からの読み取りデータを復調するためのものであり、制御回路によって復調制御がなされるようになっている。

【0036】切り替えスイッチ61(SW2)は、前記で説明した各信号処理手段から出力されたデータを選択的に各種のエラー処理手段に出力するためのものである。また、光磁気ディスク58への書き込みを行う場合には、エラー処理手段→信号処理手段への逆方向のデータの転送も制御する。

【0037】エラー処理手段は、通信系エラー処理部62と、光磁気ディスク系エラー処理部62(62a, 62b)と、磁気ディスク・CD系エラー処理部63とに分かれている。

【0038】光磁気ディスク系エラー処理部62は、エラーチェックコード生成部62aと、エラーチェックコード訂正部62bとからなり、光磁気ディスク58への書き込みを行う場合には前者が機能し、光磁気ディスク58からの読み出しを行う場合には後者が機能する。なお、磁気ディスク・CD系エラー処理部63は、エラーチェックコード訂正とともにビット並び替え等の処理も行うようになっている。

【0039】前記エラー処理手段の後段には切り替えスイッチ64(SW3)が配置されている。この切り替えスイッチ64(SW3)は、前記の信号処理手段およびエラー処理手段で処理されたソフトウェア情報を次段のソフトウェア管理部3に出力するか、後述の切り替えスイッチ65(SW4)に出力するか、あるいは前述のエラーチェックコード訂正部62bからの出力をエラーチェックコード生成部62aに戻すように経路を制御する機能を有している。

(CD-ROM→光磁気ディスクへの書き込み)ここ

で、切り替えスイッチ64(SW3)を制御して、CD-ROM52から読み込んだ暗号化ソフトウェア情報を光磁気ディスク58に書き込む手順を簡単に説明する。

【0040】まず、CD-ROM52から読み込まれたデータは、切り替えスイッチ57(SW1)の経路切り替えによりCD/MO復調器60に入力される。ここで復調されたデータは、切り替えスイッチ61(SW2)の経路切り替えにより磁気ディスク・CD系エラー処理部63に送られる。ここでエラーチェックコード訂正およびビット並び替えが行われたデータは、切り替えスイッチ64(SW3)の経路切り替えによってエラーチェックコード生成部62aに送られ光磁気ディスクに対応したエラーチェックコードが付加される。そして、このデータは切り替えスイッチ61(SW2)の経路切り替えによりMO変調器59に送られ光磁気ディスク58に書き込むことのできるデータ形式に変換されて切り替えスイッチ57(SW1)を通じて光磁気ディスク58に書き込まれる。

(ソフトウェア管理部の構成)ソフトウェア管理部3は、モジュール構造でたとえばICカード、ボード等で実現されており、入力用バッファ21と出力用バッファ24とを有する復号化部7としてのDESを中心に構成されている。ここで、DESとしては、FIP' SPU B社の「46 DATA ENCRYPTION STANDARD NIST」を用いることができる。

【0041】前記DESには外部より鍵情報16が与えられるようになっており、この鍵情報に基づいてDESが機能して暗号化情報を復号化するようになっている。なお、本実施例においてDESにはモード判別部18

(MODE)を有しており、このモード判別部18は複数のDESモードの中からそのデータ形式等に対して最適なモードを選択する機能を有している。

【0042】なお、このDESは本装置をセンタ91あるいは中継装置95として用いる場合には復号化部7(復号か処理手段95b)としての機能の他、暗号化部(暗号化処理手段95f)としても機能する。また、このときモード判別部18は入力側利用モード判別手段95cおよび出力側利用モード判別手段95eとして機能することになる。そして、制御CPU4は暗号化鍵生成手段95aおよび復号化鍵生成手段95dとして機能することになる。

(DESモードの説明)次に前記DESモードのうち、代表的なロジックを説明する。なお、以下の説明では復号化処理を中心に説明するが、本装置をセンタ91または中継装置95として使用するときには暗号化処理も下記と同様である。

【0043】図4(a)は、ECB基本モードであり、DES7において、64ビットの鍵情報16により64ビットの入力データ列を64ビットの出力データ列として暗号化(または復号化)するモードである。

【0044】図4(b)は、CBCモードを示しており、DES7において64ビットの入力データ列を64ビットの鍵情報16で暗号化(または復号化)した後、再度これをDES7に帰還入力させる。このようにデータを全て入力し終るまでフィードバックを行い最終結果を出力する方式であり、ファイル等のデータ処理に適している。

【0045】図4(c)は、OFBモードを示しており、エラーの生じやすい通信データや、一つの誤りが他に与える影響の大きい音声データ等に適している。図4(d)は、CFBモードであり、自己同期形のデータに適している。

【0046】前述のモード判別部18はモードテーブル20に格納されたこれらのモードのうらデータ形式等を解析して最適なものを読み出して復号化部(DES)に送出する。DES7ではこのようにして選択されたモードに基づいて暗号化・復号化処理を行う。

(復号化部の詳細)図5は、復号化部7のハードウェア構成を示すブロック図である。

【0047】同図において、入力側には入力用バッファ21として、8ビット構成のレジスタが8個接続されて64ビットのシフトレジスタ(REG1)が配置されており、次段にはセクタselが配置されている。当該セクタselは、後述のDES処理メイン回路25からの出力か、前記シフトレジスタ(REG1)からの出力かを選択的に入力できるようになっている。

【0048】セクタselの次段には8ビット構成のレジスタ23(REG2)が配置されさらにその次段にはDES処理メイン回路25が配置されている。このDES処理メイン回路25が復号化部7の中核をなすDESとして機能する。すなわち、DES処理メイン回路25には、図4で説明した各種のDESモードがROM(Read Only Memory)として登録されており、制御CPU4からの指示により最適なDESモードのロジックを選択して復号処理を行うようになっている。

【0049】前記DES処理メイン回路25の出力は前記セクタselと出力用バッファ24としての出力レジスタ(REG3)に分岐されている。そして出力レジスタ(REG3)の出力が暗号化または復号化されたデータとして用いられる。

【0050】この処理のシーケンスを示したものが図6である。図6において、入力レジスタ(入力用バッファ21)の出力は、次サイクルの最初のクロックでレジスタ23からの出力としてDES処理される。そして次のクロックで出力レジスタ(出力用バッファ24)より出力される。この出力レジスタ(出力用バッファ24)からの出力時間に入力側では入力レジスタ(入力用バッファ21)より次サイクルの暗号化データの取り込みが行われている。

【0051】このように、本実施例では入力用バッファ21としての入力レジスタ(REG1)と、出力用バッファ24としての出力レジスタ(REG3)とを独立に設けたことにより、暗号化データの入力と復号化データの出力とをそれぞれ独立して連続的に行うことができるようになった。そのため、従来のDESのようにサイクリックに入力と出力とを行う場合に較べて高速な復号化・暗号化処理が可能となっている。

【0052】以上説明したDES7は、制御CPU4により制御されるようになっており、この制御CPU4のバスには前記DES7の他にメモリで構成された課金テーブル8と、インターフェース72(I/O)が接続されている。

【0053】課金テーブル8には所定の残高値が登録されており暗号化ソフトウェアデータの復号処理量または処理時間に応じて課金値が減算されるようになっている。残高値を更新したい場合には、カード媒体として提供されているソフトウェア管理モジュールを販売店等に持参し、料金を支払うことにより販売店で課金テーブル8の残高値を増加させることができる。

【0054】なお、SD回路3内に課金テーブル8を設けない場合には、当該課金値情報をフロッピーディスク装置等に出力して記録しておく必要がある。この場合に課金値情報をユーザが可読な状態でフロッピーディスク等の媒体に登録しておくセキュリティが維持できない。そこで、当該課金値等情報のユーザ情報を外部に出力する場合には、前記制御CPU4はDES7で当該課金値情報を暗号化して暗号データとして出力するようにしてもよい。

【0055】すなわち、課金値情報を外部に出力する場合には復号化部(DES)は暗号化部として機能することになる。なお、本装置をセンタ91または中継装置95としてのみ使用する場合には、このような課金テーブル8は省略してよいことは勿論である。

【0056】インターフェース72(I/O)はソフトウェア管理部3外のホストCPU10と接続されている。なお、前記制御CPU4はホスト装置(すなわちソフトウェア従量課金・再生装置本体)側のホストCPU10で兼用することも可能である。

【0057】ホスト側ではホストCPU10のバス上にインターフェース(I/O)が接続されており、これと外部インターフェース75を通じて入力装置74とモデム73とが接続されている。

【0058】ソフトウェア管理部3の出力は、切り替えスイッチ65(SW4)を通じて情報変換部である音声画像分離部66(DE-MUX)、画像伸長部67a、音声伸長部67b(MPEG)等に出力される。

【0059】ここで、MPEGとしては、チップとして「ISO/IEC CD 13818' 1~3」を用いることができる。音声画像分離部66(DE-MUX)

で分離された画像データは、画像伸長部67a(MPEG)で伸長されDA変換部68aで変換されたNTSC信号としてTVディスプレイ等のアナログ表示機器に出力される。

【0060】音声伸長部67b(MPEG)でも同様に音声データが伸長されDA変換部68bで変換されたNTSC信号としてスピーカ等のアナログオーディオ機器に出力される。そして、画像と音声の同期は同期制御部70(VRC)で制御される。なお、音声画像分離部66(DE-MUX)の出力をデジタルデータままで外部に出力するときにはインターフェース71(SCSI)を通じてパーソナルコンピュータ等のデジタル機器に出力する。

【0061】なお、本装置をセンタ91または中継装置95として用いる場合でいわゆるビューワ(コンテンツを参照するツール)を必要としないときには音声画像分離部66(DE-MUX)以降の構成は省略してもよい。

(本発明におけるソフトウェアの提供ルート)図7~図9を用いて、本発明のソフトウェアの提供モードについて説明する。

【0062】図7において、センタ91からエンドユーザ121にソフトウェアが提供され得る形態としては、第1に通信事業者122を経由するルートがあり、第2にセンタ91からの直販ルートがあり、第3に販売店123を経由するルートがある。

【0063】第1の通信事業者122を経由するルートでは、センタ91から通信事業者122までは通信路C1でソフトウェアが提供される場合と、媒体形式P1でソフトウェアが提供される場合がある。通信路C1としては、公衆回線、光通信路、衛星通信等のあらゆる通信手段を想定することができる。媒体形式P1としてはCD-ROM、光磁気ディスク、ハードディスク、フロッピーディスク等のあらゆる媒体手段を想定することができる。

【0064】このルートにおいて、通信事業者122からエンドユーザ121までは通信経路C2でソフトウェアが提供される。このルートでセンタが通信事業者122に対してソフトウェアを提供する場合には、まず通信路C1の場合には暗号化モードとして図4(c)に示したOFBモードが最も適している。したがって、センタ91は自身のDES7によってOFBモードによる暗号化データを生成し、これを通信路C1に出力する。

【0065】通信路C1から暗号化データを受け取った通信事業者122は自身の中継装置95を用いて受信した暗号化データをそのまま通信路C2に出力する(図9(a))。通信路C2から暗号化ソフトウェアデータを受け取ったユーザ端末92の処理は先に説明した通りである。

【0066】次に、センタ91から媒体形式で通信事業

者122に暗号化ソフトウェアデータが送られる場合について説明する。媒体形式P1の場合には暗号化モードは図4(b)に示したCBCモードが最適である。したがって、センタ91は自身のDES7においてCBCモードでソフトウェアデータを暗号化してCD-ROM等の媒体にこのデータを格納する。このように暗号化ソフトウェアデータがCD-ROM等の媒体に格納された状態でこれを受領した通信事業者122は、この暗号化ソフトウェアデータを通信路C2に供給するために、自身のDES7を用いて暗号化モードの変換を行う(図9(b)参照)。すなわち、先に述べたように通信路C2に流通させる暗号化モードとしてはOFBモードが適しているため、まず受領した暗号化ソフトウェアデータをCBCモードで復号した後、OFBモードで再暗号化する。このように暗号化された暗号化ソフトウェアデータを受領したエンドユーザ121は、自身のユーザ端末92のDES7で、モード判別部18(MODE)で選択されたOFBモードに基づく復号を実行する。

【0067】次に、販売店123を経由したソフトウェアの流通形態について説明する。まずセンタ91から販売店123までが通信路C3で結ばれており、販売店123からエンドユーザ121へは媒体形式P2での提供である場合、センタ91は自身のDES7においてOFBモードで暗号化した暗号化ソフトウェアデータを通信路C3に送出する。

【0068】販売店123では自身の中継装置95でこれを受信して光磁気ディスク等の媒体(P2)にこの暗号化ソフトウェアデータを格納する(図9(c))。この媒体(P2)の提供を受けたエンドユーザ121のユーザ端末92では、自身のDES7においてOFBモードで当該暗号化ソフトウェアデータの復号処理を行う。

【0069】以上の中継装置95におけるモード変換の一覧を示したものが図8である。すなわち、以上の説明はいずれも流通方向が片方向(センタ91からエンドユーザ121へ)のみであったが、双方向の場合には全てCBCモードを採用することが望ましい。

【0070】

【発明の効果】本発明によれば、ソフトウェアの提供形態に最適なモードを選択して暗号化・復号化処理を流通経路上で行うようにしたため、ソフトウェア格納媒体の販売者と、通信回線を利用してソフトウェアを提供する通信事業者とを含めたソフトウェアの流通形態を実現することができる。

【図面の簡単な説明】

【図1】 本発明の原理図(1)

【図2】 本発明の原理図(2)

【図3】 本発明の実施例であるセンタ、中継装置、ユーザ端末のハードウェア構成を示す機能ブロック図

【図4】 DESのモードを示す説明図

【図5】 DESの詳細を示す説明図

【図 6】 DES の入力と出力のタイミングを示すチャート図

【図 7】 本発明のソフトウェアの提供経路を示す説明図

【図 8】 提供経路毎のモード変換を示す表図

【図 9】 実施例における中継装置でのモード変換を説明するための概念図

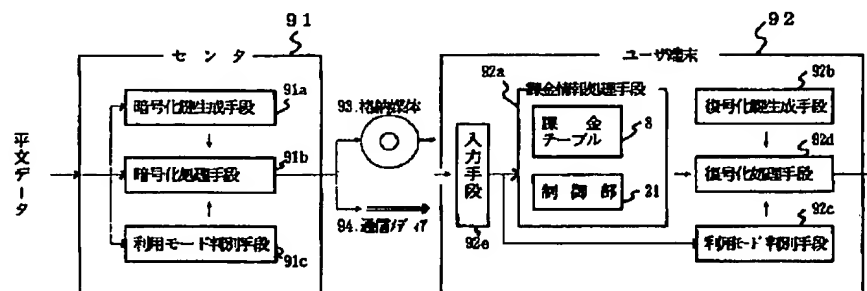
【符号の説明】

3・・・ソフトウェア管理部、
4・・・制御 CPU
7・・・DES（復号化部、暗号化部）
8・・・課金テーブル、
10・・・ホスト CPU
16・・・鍵情報、
18・・・モード判別部、
20・・・モードテーブル、
21・・・入力用バッファ、
24・・・出力用バッファ、
51・・・通信回線、
57・・・切り替えスイッチ、
58・・・光磁気ディスク、
59・・・MO変調器、
60・・・CD/MO復調器、
61・・・切り替えスイッチ、
62・・・通信系エラー処理部、
62a・・・エラーチェックコード生成部、
62b・・・エラーチェックコード訂正部、
63・・・磁気ディスク・CD系エラー処理部、
64・・・切り替えスイッチ、
65・・・切り替えスイッチ、
66・・・音声画像分離部、
67a・・・画像伸長部、

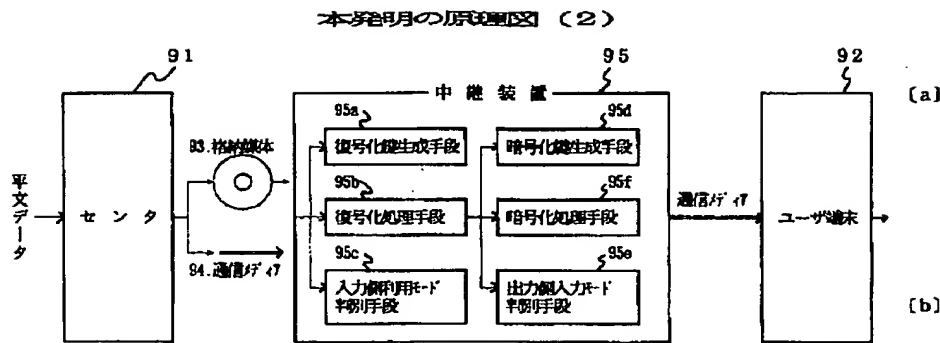
* 67b・・・音声伸長部、
68a・・・DA変換部、
68b・・・DA変換部、
70・・・同期制御部、
71・・・インターフェース、
72・・・インターフェース、
73・・・モデム、
74・・・入力装置、
75・・・外部インターフェース、
10 79・・・受信装置、
91・・・センタ、
91a・・・暗号化鍵生成手段、
91b・・・暗号化処理手段、
91c・・・利用モード判別手段、
92・・・ユーザ端末、
92a・・・課金情報処理手段、
92b・・・復号化鍵生成手段、
92c・・・利用モード判別手段、
92d・・・復号化処理手段、
20 920・・・入力装置、
93・・・格納媒体、
94・・・通信メディア、
95・・・中継装置、
95a・・・復号化鍵生成手段、
95b・・・復号化処理手段、
95c・・・入力側利用モード判別手段、
95d・・・暗号化鍵生成手段、
95e・・・出力側利用モード判別手段、
95f・・・暗号化処理手段、
30 102・・・ソフトウェア管理モジュール、
105・・・ソフトウェア従量課金・再生装置、
* 921・・・制御部、

【図 1】

本発明の原理図 (1)



【図 2】

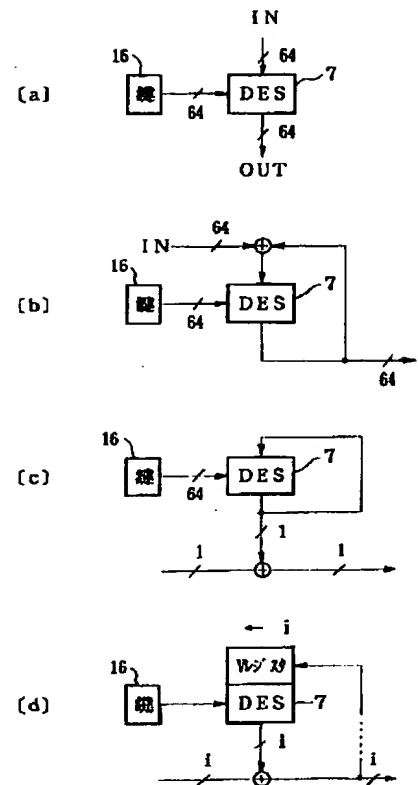


【図 8】

提供経路毎のモード変換を示す表

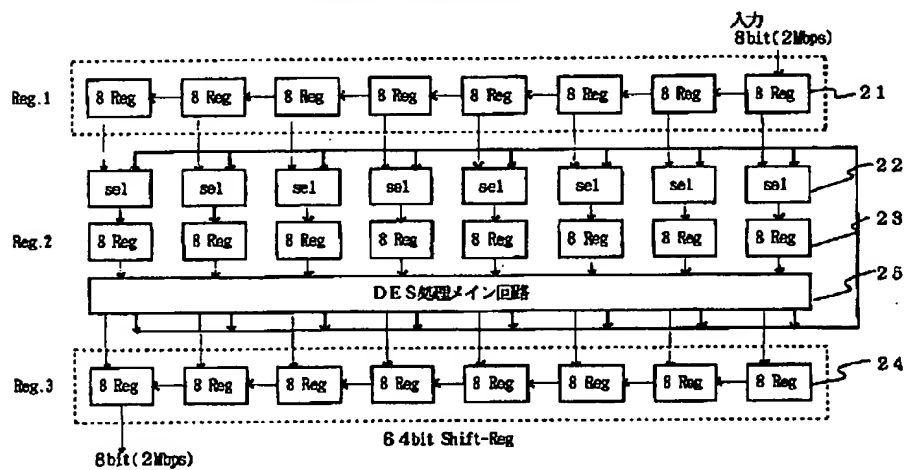
方式	モード	C1→C2	P1→C2	C4	C3→P2	P4及びP3→P2
片方向		OFB→OFB	CBC→OFB	OFB	OFB→OFB	CBC→CBC
双方向		CBC→CBC	CBC→CBC	CBC	CBC→CBC	CBC→CBC

【図 4】

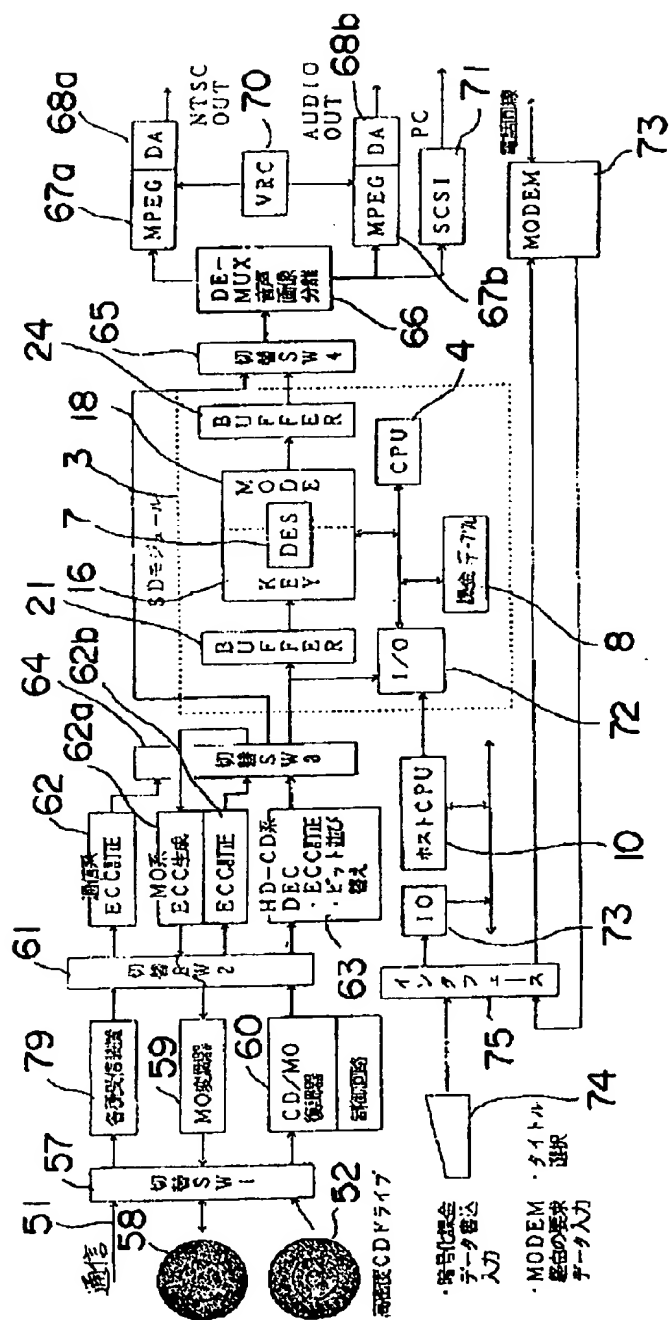


【図 5】

実施例のDESの詳細な構成を示すブロック図

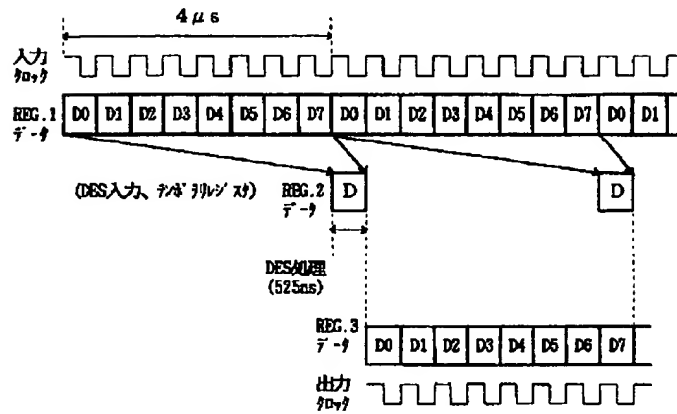


【図 3】



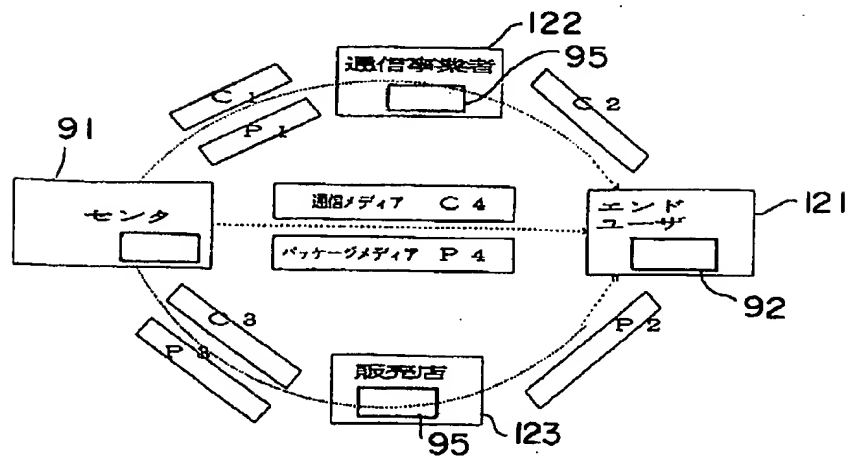
【図 6】

実施例のDESの入力と出力とのタイミングを示すチャート図

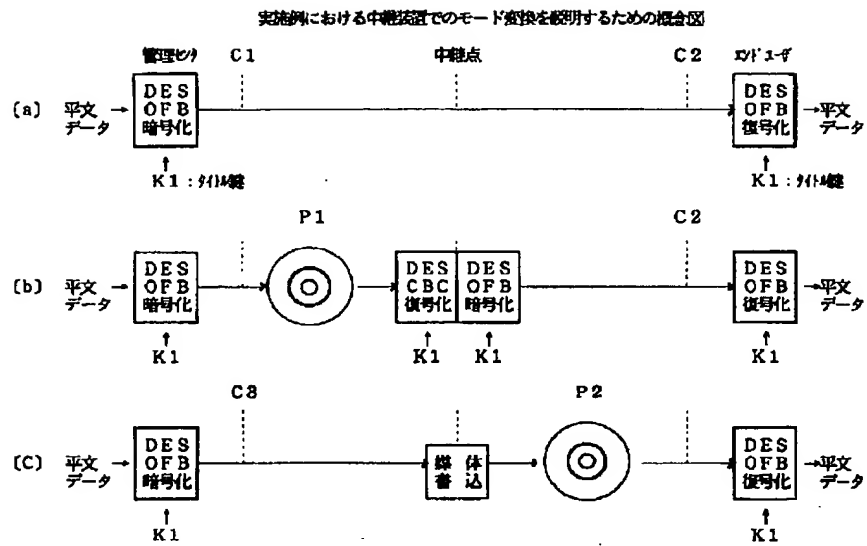


【図 7】

本発明のソフトウェアの提供経路を示す説明図



【図 9】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.